~~CONFIDENTIAL~~

ROUTING AND RECORD SHEET

SUBJECT: (Optional)
Interagency Group/Countermeasures

STAT FROM:
STAT C/ISSG/OS

EXTENSION | NO.

DATE
26 MAY 1983

TO: (Officer designation, room number, and building)	DATE RECEIVED	DATE FORWARDED	OFFICER'S INITIALS	COMMENTS (Number each comment to show from whom to whom. Draw a line across column after each comment.)
STAT 1. C/PPG [redacted] 4E70 Hqs.				
2.				
3.				
4.				
5.				
6.				
7.				
8.				
9.				
10.				
11.				
12.				
13.				
14.				
15.				

FORM 610 USE PREVIOUS EDITIONS
1-79

~~CONFIDENTIAL~~

26 MAY 1983

MEMORANDUM FOR: Chief, Policy and Plans Group

STAT ATTENTION: [redacted]

STAT FROM: [redacted]
Information Systems Security Group

STAT SUBJECT: Interagency Group/Countermeasures [redacted]

REFERENCE: Memo for Members and Invitees from IG/CM, dated 10 May 83, same Subject, D/ICS-83-0676

1. The Navy candidate issue concerning "National Policy on ADP Security" presents an excellent opportunity for the Intelligence Community and the USG in general to standardize computer security policy and countermeasures throughout the
STAT Government. [redacted]

2. As you are aware, the Computer Security Subcommittee under SECOM is now revising the DCID titled "Security of Foreign Intelligence in Automated Systems and Networks." This document will address both Sensitive Compartmented Information and collateral intelligence information. It could well prove to be adaptable, at least in part, to all areas of USG interest. It should, at a minimum, be a good base for an overall
STAT USG policy in the computer security field. [redacted]

STAT [redacted]

STAT [redacted]

STAT [redacted]

ROUTING AND RECORD SHEET

SUBJECT: (Optional)
Interagency Group/Countermeasures

STAT
PPG/OS
STAT 4E-70, HQS

EXTENSION | NO.

DATE 13 May 1983

TO: (Officer designation, room number, and building)	DATE RECEIVED	DATE FORWARDED	OFFICER'S INITIALS	COMMENTS (Number each comment to show from whom to whom. Draw a line across column after each comment.)
1. C/TSSG STAT				STAT Here's the latest IG/CM material. Warren already has a copy of STAT Organizational Study. You'll be especially interested in the Navy's Candidate Issues for IG/CM consideration... particularly Item 3. I thought SECOM had the con on that item, and that you folks were and are well ahead of the rest of the world in that area. Since STAT is supposed to vote for or against IG/CM consideration of these items, your thoughts would be much appreciated. Please feel free to comment on anything you see in this package, even if it's not ISSG-related. Thanks.
2. STAT				
3.				
4.				
5.				
6. STAT				
7.				
8.				
9.				
10.				
11. STAT				STAT
12.				
13.				
14.				
15.				

FORM 1-79 610 USE PREVIOUS EDITIONS

Interagency Group/Countermeasures

Washington, D.C. 20505

D/ICS-83-0676
10 May 1983

MEMORANDUM FOR: Members and Invitees

STAT FROM: [redacted]
Executive Secretary

STAT SUBJECT: Interageny Group/Countermeasures (IG/CM)
Administrative Actions [redacted]

1. The final minutes of the fourth IG/CM meeting are enclosed as Attachment 1. Addressees are requested to examine the minutes and complete
STAT assigned actions as required. [redacted]

2. The fifth meeting of the IG/CM will be held on Friday, 3 June 1983, at 1400 hours. The meeting will convene in Rm. 6744, Department of Justice, 10th and Pennsylvania Avenue, N.W., Washington, D.C. Seating space in the DoJ secure conference room is limited; therefore, attendance at this particular meeting should be restricted to the minimum required to address agenda
STAT items. [redacted]

a. The meeting agenda is enclosed as Attachment 2. Addressees have already received materials pertinent to all issues listed in paragraph 2 of the agenda except for the draft industrial security policy memorandum, which is enclosed as Attachment 3. It is anticipated that the status reports reflected in paragraph 3 of the agenda will be limited to 2-3
STAT minutes each. [redacted] STAT

b. Members and invitees are requested to call [redacted] STAT
[redacted] by COB 31 May with the names of individuals who will be
STAT attending the meeting. [redacted]

3. NSA has submitted a proposed new issue for IG/CM consideration, which is enclosed as Attachment 4. Addressees are requested to prepare respective agency comments/positions on the proposal for discussion at the 3 June
STAT meeting. [redacted]
STAT

[redacted]

Attachment:
a/s

DS REGISTRY
83-1132/1

STAT [redacted] [redacted] STAT

CONFIDENTIAL

SUMMARY OF IG/CM MEETING

14 APRIL 1983

1. The fourth IG/CM meeting was convened at 1400 hours, 14 April 1983, STAT by the Chairman (DUSD-Policy), General Richard G. Stilwell, USA (Ret.). A listing of individuals attending is attached.

2. General Stilwell advised the membership that on 11 March 1983 the SIG(I) had approved the IG/CM paper on Foreign Civil Overflights of the U.S. and had forwarded it to the NSC for further action. He also advised that the IG/CM-approved report on Unauthorized Disclosures had been signed by the President as NSDD-84. The NSC is involved in working groups which are ironing out implementation procedures. The Chairman reported he had provided the Senate Select Committee on Intelligence (SSCI) with a status update on issues the IG/CM is currently considering and that the SSCI seemed pleased with the extent of IG/CM involvement. General Stilwell commented on the French Government expulsion of 47 Soviets for reported involvement in intelligence activities (technology transfer) and observed that the incident will hopefully STAT have a beneficial effect in the U.S.

3. The Chairman invited attention to the agenda and called for status reports on listed issues:

a. Foreign Civil Overflights. The Chairman recalled his opening STAT remarks and suggested that Mr. deGraffenreid, NSC representative, keep the membership posted on the paper's status in the NSC.

STAT Action: Mr. deGraffenreid is to report on the overflight paper status at the next IG/CM meeting.

b. Unauthorized Disclosures. Mr. deGraffenreid reported on progress of the task to develop implementing procedures for NSDD-84. Essentially, there are four segments being examined. Steve Garfinkle of the ISOO is chairing a group examining the prepublication review aspect and other forms. This group has identified a number of policy questions and is seeking the appropriate channel for their resolution. A Media Contacts Group led by Bob Simms is just starting its tasks. The two remaining groups are led by DoJ. The Unauthorized Disclosure Investigative Procedures Group is examining the criteria the FBI will use to initiate unauthorized disclosure investigations. It is also working with OPM on the polygraph issue. The fourth group is examining the Federal Personnel Security Program. It is, therefore, doubtful that implementing drafts will be ready by the 18 April deadline. Mr.

CONFIDENTIAL

ATTACHMENT 1

STAT deGraffenreid noted that a number of new investigations are being called for under the thrust of NSDD-84.

Action: The NSC representative will keep the IG/CM apprised of significant developments concerning the development of implementing procedures for NSDD-84. Another status report is requested at the next
STAT IG/CM meeting.

c. OPSEC. The OSD representative, Mr. Snider, distributed an OPSEC policy paper which integrates all member comments received to date. State is to take a final look at the paper and provide concurrence decision by not later than 18 April. All other members concurred with the paper.

Action: The IG/CM Secretariat is to forward the OPSEC paper to
STAT the SIG(I) subsequent to noon, 18 April, monitor its status, and report as necessary to the IG/CM membership.

d. Fourth Level of Classification. Mr. Snider advised he had discussed the "Confidential Modified Handling Authorized" (CMHA) classification possibility with ISOO as promised. ISOO, while agreeing that such a classifiction could be implemented with modification of the ISOO Directive, opposed doing so. The principal objections were the probable confusion which would result and the adverse impact it would have on Defense contractors. Mr. Snider distributed a related study done by Mr. Art Van Cook and advised that the ISOO Director has recommended its conclusions as an alternative to the CMHA approach. The study suggests each agency protect sensitive information through implementation of its own internal controls and offered a way in which DoD could accomplish this. Mr. Snider indicated OSD would like to put the fourth classification issue on hold until DoD evaluates the Van Cook approach more thoroughly. He advised the Van Cook study reportedly takes the legal (FOIA) aspect into consideration. The Army (Col. Press) and Air Force (Mr. Paseur) representatives responded to the Chairman's request for comments. They indicated they still strongly support having a fourth classification and have great concerns about industry/contractor adherence to the "internal" controls concept, but will examine the Van Cook study. Mr. Snider advised that on 21 April the Senate Judiciary
STAT Committee will consider the legislative action the IG/CM recommended to exempt technical data from FOIA provisions.

Action: Members are to examine the Van Cook study and prepare
STAT to comment on it as an alternative to the fourth classification proposal. DoD is to coordinate its position.

e. Damage Assessments. The SECOM representative, Mr. Paschal, introduced a paper distributed to members via IG/CM Secretariat memorandum dated 7 April 1983. After summarizing the various options for

a lessons learned data base, he recommended one of the options be chosen, that it be limited to intelligence compromises only, and that a pilot study be conducted to determine how well it meets the needs. General discussion followed on the cost of a pilot program--estimated at $200,000 over a one-year period, what purposes a data base would/should serve, and what ingredients should make up the data base. The Justice representative, Ms. Lawton, pointed out two problems: If the data base contained names of individuals on dissemination lists, we would have a Privacy Act problem; if CIA holds the data base files on compromises which are the subject of ongoing criminal investigations, this could raise a question of CIA involvement in domestic law enforcement. State and Defense objected to the inclusion of names in the data base. DoD further observed that their attempt to construct a similar type data base yielded questionable results. A review was given of why the issue of damage assessment was before the IG/CM, what the task has been to SECOM,
STAT and where we now stand.

Action: The Chairman asked members to examine options (1) and (2) of the SECOM paper. Members are to identify, in writing for each option, what individual agency preferences are for: (1) the purposes of a lessons learned data base, e.g., what it is hoped the data base will accomplish/permit; (2) what input elements the data base should contain to accomplish the purposes; and (3) any specific input elements the agency would not support in a damage assessment lessons learned data base. These items will be discussed at the IG/CM meeting and subsequently provided to SECOM for reconstruction of a second strawman.
STAT

f. Industrial Security. Mr. Snider reported the results of his research into the best vehicle for national level promulgation of the FOCI provision of the DoD Industrial Security Regulation. A National Security Council Policy Memorandum was the vehicle recommended to and
STAT approved by the membership.

Action: DoD will prepare a draft policy memorandum on Industrial Security and arrange for its timely distribution so that
STAT members can comment/concur at the next meeting.

g. Personnel Security. The DoJ representative, Mr. Cinquegrana, advised that the new NSDD-84 specifies that DoJ will chair the research into implementation procedures for personnel security aspects of that Directive. Since DoJ representatives had previously deliberated with the IG/CM working group on personnel security, DoJ will look into incorporating the conclusions of the IG/CM group into NSDD-84 actions. DoJ is considering different approaches to the project, including the option of two subgroups chaired by OPM and DoD respectively. A final approach, however, will not be decided upon until initial consultations are completed with DoD and OPM.

Action: DoJ will continue to work the personnel security issue as chartered by NSDD-84, and DoD representatives, working with DoJ, will push for incorporation of the IG/CM working group's conclusions into
STAT national policy documents.

STAT h. COMSEC Monitoring. The NSA representative, advised that a draft of NACSI 4000 had been out for comment since February 1983. The civil sector had no comments but the Military Services, with Navy leading, had several. He opined that rewording of the draft, in coordination with DoJ, will resolve problems and that a final draft could
STAT be out by May.

Action: NSA is to continue to push for earliest completion of the final draft and advise the IG/CM of significant problems if they
STAT occur.

i. Organizational Study. Mr. Jason Horn, Study Director, advised that a final draft of the Organizational Study would be out to members by 10 May. A minimum of two weeks will be required for field comment, and subsequent drafts are anticipated. As a result, it was determined that the SIG(I) Chairman be advised that it is unlikely the study will be
STAT completed by 31 May.

Action: The IG/CM Chairman will advise the SIG(I) Chairman of the slip in completion date. Mr. Horn will continue efforts to expedite completion of the study and advise of significant problems if they
STAT occur.

j. TEMPEST Policy. The NSA representative advised that the Subcommittee on Compromising Emanations (SCOCE) has been working on alternatives for TEMPEST policy. A draft revision of CONUS TEMPEST Standards is to reflect considerable relaxation of current requirements. Overseas requirements are to remain high. The Chairman suggested deferral of discussion on this issue until completion of the Organizational Study since the study will also address TEMPEST
STAT considerations.

Action: IG/CM action on this issue will be held in abeyance until completion of the Organizational Study.

k. Security Enhancement of U.S. Embassies. The Chairman discussed SIG(I) reaction to this subject when surfaced at its 11 March meeting. The results of that meeting, as well as a DIA position paper distributed to members at the instant IG/CM meeting, caused the Chairman to suggest the need for redefinition of the problem the IG/CM needs to consider. The Chairman asked that State chair a working group composed of State, DIA, CIA and NSA members, at a minimum, to accomplish a reexamination of
STAT the problem and to report findings to the membership.

Action: State is to identify a chairperson and call a meeting of appropriate representatives to reconsider what aspect(s) of the security of U.S. embassy problem the IG/CM needs to address. The principal guide in this review is to be pertinent portions of Chapter VII in the study, "Capabilities Against the Hostile Intelligence Threat, 1983-1988." STAT

4. The Chairman opened the floor to discussion of new issues for IG/CM consideration:

a. Both DoD and State suggested that knowledge of the background, methodology, and purpose of the recent French Government expulsion of Soviet diplomats would provide beneficial lessons learned data to Intelligence Community members. STAT

Action: IG/CM Secretariat is to coordinate with CIA on the possibility of a briefing on the subject and report to IG/CM members at the next meeting. STAT

b. The Navy representative, Captain Hoskins, passed out a list containing five proposed issues (attached). The Chairman asked the membership to review the proposed issues and prepare their views on acceptability for IG/CM consideration. STAT

5. The meeting adjourned at 1550 hours. STAT

DEPARTMENT OF THE NAVY CANDIDATE ISSUES FOR THE INTERAGENCY GROUP/COUNTERMEASURES

1. (U) National Policy on Use of the Polygraph. A number of individual initiatives have been launched in this area; the cumulative effect of these possibly disparate efforts needs to be examined and a national policy developed.

2. (U) National Policy on Anticompromise Emergency Destruct (ACED). A new family of equipment is being developed by the Navy which will permit the anticompromise emergency destruction of sensitive information and equipment. However, lack of a national policy and appropriate funding may limit the effective development of the new ACED devices.

3. (S) National Policy on ADP Security. At present there appears to be considerable differences in the application of ADP security measures. This is of particular concern since it appears that ADP security vulnerabilities are targeted for exploitation by hostile intelligence services.

4. (C) National Policy on Secure Telephones. The loss of sensitive information in non-secure telephone conversations is a major security problem which may be solved only by high-level support for greater availability and use of secure communications equipment.

5. (U) Definition of Unclassified National Security Information. Certain national policy now requires that such information be protected; in order to protect this information, it must first be defined and protective thresholds established.

Classified by: Multiple Sources
Declassify on: OADR

CONFIDENTIAL

ATTENDEES

IG/CM Meeting, 14 April 1983
Room 6W02, Community Headquarters Building

NAME	ORGANIZATION
Richard G. Stilwell, Chairman	OSD
L. Britt Snider	OSD
Edwin Yee	FBI
STAT	CIA
	CIA
	CIA
Donald Macdonald	State
Thomas McCay	State
STAT	NSA
	NSA
Kenneth deGraffenreid	NSC
STAT	DIA
	DIA
	DIA
Donald Press	Army
Frank Aurelio	Army
P. D. Hoskins	Navy
George W. Paseur	Air Force
John J. Guenther	Marine Corps
Donald Paschal	SECOM
Ed Cohen	SECOM
Mary C. Lawton	Justice
A. R. Cinquegrana	Justice
J. Robert McBrien	Treasury
Mike Cassetta	Commerce
Robert Wingfield	Energy
Douglas Miller	Energy
IC Staff Attendees	
STAT	CCIS/ICS
	CCIS/ICS
	CCIS/ICS
	IG/CM Staff
	IG/CM Staff
	IG/CM Staff

CONFIDENTIAL

AGENDA

Fifth IG/CM Meeting
3 June 1983

1. Chairman's Opening Remarks

2. Discussions:

   a. Review of DoD-prepared industrial security policy memorandum. Member concurrence decision.

   b. Review of agency inputs to damage assessment lessons learned data base issue. Course of action decision.

   c. Review of Navy-proposed IG/CM issues. Decision on acceptability. Assignment of action as appropriate.

   d. Review of NSA-proposed IG/CM issue. Decision on acceptability. Assignment of action as appropriate.

3. Status Reports:

   a. Overflight policy paper -- NSC representative

   b. NSDD-84 -- NSC and DoJ representatives

   c. NACSI-4000 -- NSA representative

   d. Embassy security enhancement working group -- State representative

   e. Countermeasure organizational study -- CCIS representative

   f. French expulsion briefing -- CCIS representative

ADMINISTRATIVE NOTE:

The IG/CM Chairman has accepted DoJ's offer to host the fifth IG/CM meeting at the new DoJ secure conference facility. Attendees will find use of the DoJ entrance at 10th and Pennsylvania Avenue the most convenient for access to Room 6744. (Sixth floor; left off elevator to first corridor. For additional directions once in the DoJ building, if needed, call Barbara, 633-3738.)

CONFIDENTIAL

ATTACHMENT 2

OFFICE OF THE UNDER SECRETARY OF DEFENSE
WASHINGTON, D.C. 20301

9 MAY 1983

POLICY

MEMORANDUM FOR THE EXECUTIVE SECRETARY, INTERAGENCY GROUP/ COUNTERMEASURES

SUBJECT: Draft NSC Memorandum Industrial Security

At the 14 April meeting of the IG/CM, it was agreed that the proposed national policy statement in the area of industrial security -- dealing with the ownership of U.S. firms by foreign interests -- would be placed in the form of an NSC memorandum, rather than as an amendment to E.O. 12356 or ISOO Directive No. 1.

Accordingly, the proposed memorandum has been prepared, incorporating what had previously been agreed to by the IG/CM without objection. Request that copies be provided IG/CM members in advance of the next meeting, so that this memorandum may be considered for transmittal to the SIG-I.

L. Britt Snider

L. Britt Snider
Director for Counterintelligence
and Security Policy
OSD Member

Attachment 1
Proposed Memorandum

ATTACHMENT 3

NATIONAL SECURITY AGENCY

FORT GEORGE G. MEADE, MARYLAND 20755

Serial: N/0582
26 April 1983

MEMORANDUM FOR THE EXECUTIVE SECRETARY, IG/CM

SUBJECT: Proposed New Agenda Item

1. Enclosed for consideration as an IG/CM agenda item is an issue paper on cryptographic access requirements and an associated proposed NSDD entitled "Safeguarding Cryptographic Information and Material."

2. The National Security Agency believes a formal cryptographic access program is the key element in our efforts to counter the HUMINT threat to U.S. cryptography. Pursuing the initiative begun in NSDD-84, our proposed NSDD would establish a national cryptographic access program based on several criteria, including a requirement for consent to aperiodic, limited polygraph examinations.

3. I recommend the enclosure be circulated to the members for discussion at our next meeting.

HAROLD E. DANIELS, JR.
NSA Representative, IG/CM

Encl:
a/s

Attach. 4

Issue Paper

Cryptographic Access Requirements

1. Prior to August 1973, a formal cryptographic access program was a national requirement. In addition to restricting access to classified cryptographic information to U.S. citizens with appropriate clearance and the need-to-know, the program required: (a) formal indoctrination stressing the unique nature of cryptographic information, its criticality, the special security regulations governing its handling and protection, and the penalties prescribed for its willful disclosure; and (b) formal records of all individuals granted cryptographic access.

2. In August 1973, the requirements for the formal indoctrination and recordkeeping were discontinued, effectively ending the formal cryptographic access program. This was done primarily to eliminate the administrative burden for military users of codes and secure voice equipments in Vietnam. In the succeeding decade, there has been a steady increase in insecurities involving cryptographic information and materials. The increased incidence of insecurities is damaging to the national security. Although it is attributable in some measure to the proliferation of cryptographic information and materials, the nature of the insecurities indicates a more serious cause, a lack of appreciation for protecting cryptography. This, in turn, is linked to the lack of a formal indoctrination requirement. Furthermore, the lack of formal records hampers the conduct of studies and investigations of insecurities and unauthorized disclosures. Additionally, the lack of signed access statements weakens prosecution in espionage cases.

3. While the foregoing are serious concerns, the greatest concern which the proposed cryptographic access program is directed toward is the HUMINT threat from cognizant agents. The key element of this program is the aperiodic, limited polygraph examination. We believe it is the most effective measure for detecting properly cleared individuals who have given or sold classified cryptographic information to unauthorized individuals. There are sufficient cases on record to give cause for grave concern. An equally important aspect of the aperiodic, limited polygraph examinations is their value in deterring individuals who have access and who might otherwise be inclined to give or sell classified cryptographic information to unauthorized individuals.

4. There is ample justification for reinstituting the proposed cryptographic access program with the added requirement for consent to aperiodic, limited polygraph examinations. The proposed NSDD (attached) is considered an appropriate means of accomplishing this, particularly in view of the recently issued NSDD-84, "Safeguarding National Security Information," which also addresses the use of the polygraph to safeguard classified national security information.

Encl:
a/s

Proposed National Security Decision Directive

Safeguarding Cryptographic Information and Material

Cryptography is especially sensitive because it is used to protect highly classified and critical information on almost every conceivable subject related to the operations and plans of the U.S. Government. For this reason, cryptographic information and materials are highly prized targets of hostile intelligence activities and must be strictly safeguarded. Access to cryptography, therefore, must be restricted to the greatest extent practicable and be consistent with national security needs. Accordingly, I direct that a cryptographic access program be established within each Federal department and agency which holds or uses cryptographic information or materials, consistent with the following:

a. Access to information which reveals the design of a classified cryptographic logic, its theory of operation, or access to classified cryptographic keying variables designated "CRYPTO" may be granted only when:

(1) The need for such access is established as necessary to perform official duties by, for, or on behalf of the U.S. Government.

(2) The individual requiring such access is a U.S. citizen, a non-U.S. citizen member of the U.S. military services, or a non-U.S. citizen employee of the U.S. Government.

(3) The U.S. Government has granted the individual a final security clearance.

(4) The individual has completed an indoctrination covering: 1) the sensitivity of cryptographic information and materials; 2) the rules for safeguarding such information and materials; 3) the rules pertaining to foreign contacts, visits, and travel; 4) the rules and procedures for reporting insecurities of COMSEC materials; and 5) the laws pertaining to espionage.

(5) The individual has executed a security agreement. All such agreements shall, at a minimum, provide for:

(a) Prepublication review to ensure deletion of classified cryptographic and any other classified information from information or materials to be disclosed.

(b) The individual's consent to participate in aperiodic, limited polygraph examinations consisting solely of questions related to disloyal activities and espionage when so required.

(c) The individual's acknowledgment of the sensitivity of, and obligation to protect, cryptographic information and materials.

Enclosure

(d) The individual's acknowledgment of his/her obligations to comply with applicable regulations governing unofficial foreign travel and contact with representatives of foreign governments.

All such agreements shall be in a form determined by the Department of Justice to be enforceable in a civil action brought by the United States and consistent with the standards developed by the Director, Information Security Oversight Office (ISOO), to satisfy these requirements.

b. In support of the cryptographic access program, the heads of Federal departments and agencies are responsible for:

(1) Restricting access to classified cryptographic information and classified cryptographic keying variables designated "CRYPTO" only to those persons who have been formally granted cryptographic access for the conduct of official business.

(2) Formally granting cryptographic access only when all the criteria set forth herein are met and maintaining records of individuals granted cryptographic access.

(3) Developing programs for the aperiodic, limited polygraph examination of personnel granted access; administering the polygraph programs; and evaluating the results of polygraph examinations. Departments and agencies with substantial polygraphing resources are encouraged to extend these resources to other departments and agencies whose limited requirements do not justify the acquisition of separate polygraphing resources.

(4) Establishing a quality control review over their respective polygraph programs to ensure the propriety of polygraph examinations, consistent with paragraph a.(5), above, and to protect individuals' rights.

(5) Reporting to the FBI and other appropriate investigative agencies information which indicates possible espionage or other unlawful activities involving classified cryptographic information or materials. Promptly advising the Director, NSA, of such incidents; the Director, NSA, will provide technical assistance as needed in the investigation of such incidents.

(6) Incorporating into contracts, where necessary, and ensuring compliance with the special security requirements associated with access to cryptographic logic, cryptographic design information, theory of operation, or cryptographic keying variables designated "CRYPTO."

(7) Recognizing the cryptographic access authorizations granted to individuals by other departments and agencies.

c. The Secretary of Defense, as Executive Agent for Communications Security, is directed to promulgate or revise national communications security policies and directives, as necessary, to implement the cryptographic access program described herein. These policies and directives will be promulgated through the national communications security issuance system.

DEPARTMENT OF THE NAVY CANDIDATE ISSUES FOR THE INTERAGENCY GROUP/COUNTERMEASURES

1. (U) National Policy on Use of the Polygraph. A number of individual initiatives have been launched in this area; the cumulative effect of these possibly disparate efforts needs to be examined and a national policy developed.

2. (U) National Policy on Anticompromise Emergency Destruct (ACED). A new family of equipment is being developed by the Navy which will permit the anticompromise emergency destruction of sensitive information and equipment. However, lack of a national policy and appropriate funding may limit the effective development of the new ACED devices.

3. (S) National Policy on ADP Security. At present there appears to be considerable differences in the application of ADP security measures. This is of particular concern since it appears that ADP security vulnerabilities are targeted for exploitation by hostile intelligence services.

4. (C) National Policy on Secure Telephones. The loss of sensitive information in non-secure telephone conversations is a major security problem which may be solved only by high-level support for greater availability and use of secure communications equipment.

5. (U) Definition of Unclassified National Security Information. Certain national policy now requires that such information be protected; in order to protect this information, it must first be defined and protective thresholds established.

Classified by: Multiple Sources
Declassify on: OADR

CONFIDENTIAL

Tab B